

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor: : **Yoshihiro ODA**  
Filed : **Concurrently herewith**  
For : **AUTHENTICATION METHOD AND....**  
Serial No. : **Concurrently herewith**

July 30, 2003

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**PRIORITY CLAIM AND**  
**SUBMISSION OF PRIORITY DOCUMENT**

S I R:

Applicant hereby claims priority under 35 USC 119 from **Japanese** patent application number **2002-243577** filed **August 23, 2002**, a copy of which is enclosed.

Respectfully submitted,



---

Thomas J. Bean  
Reg. No. 44,528

Katten Muchin Zavis Rosenman  
575 Madison Avenue  
New York, NY 10022-2585  
(212) 940-8800  
Docket No.: FUJI 20.527

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 8月23日

出 願 番 号

Application Number:

特願2002-243577

[ST.10/C]:

[JP2002-243577]

出 願 人

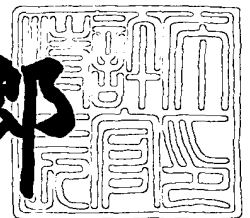
Applicant(s):

富士通株式会社

2003年 1月17日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

太田信一郎



出証番号 出証特2002-3107067

【書類名】 特許願

【整理番号】 0251039

【提出日】 平成14年 8月23日

【あて先】 特許庁長官 太田 信一郎 殿

【国際特許分類】 G06F 15/00

【発明の名称】 認証方法及びその装置

【請求項の数】 5

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 小田 美博

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100070150

【住所又は居所】 東京都渋谷区恵比寿4丁目20番3号 恵比寿ガーデンプレイスタワー32階

【弁理士】

【氏名又は名称】 伊東 忠彦

【電話番号】 03-5424-2511

【手数料の表示】

【予納台帳番号】 002989

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0114942

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 認証方法及びその装置

【特許請求の範囲】

【請求項 1】 複数の W e b サーバで特定の利用者グループにアクセスを制限するための認証方法において、

クライアント端末から前記特定の利用者グループにアクセスを限定した自装置のアクセス制限領域へのアクセス要求を受けた認証情報を持たない第 1 W e b サーバは、前記特定の利用者グループにアクセスを限定したアクセス制限領域を持ち認証情報を登録した第 2 W e b サーバに対し認証依頼を行い、

前記第 2 W e b サーバからの認証結果を受けた前記第 1 W e b サーバは、前記認証結果に応じて前記クライアント端末からの前記アクセス制限領域のアクセスを行わせることを特徴とする認証方法。

【請求項 2】 請求項 1 記載の認証方法において、

前記第 2 W e b サーバからの認証情報要求を受けた前記第 1 W e b サーバは、前記認証情報要求を前記クライアント端末に渡し、

前記認証情報要求に対する前記クライアント端末からの認証情報を受けた前記第 1 W e b サーバは、前記認証情報を前記第 2 W e b サーバに渡すことを特徴とする認証方法。

【請求項 3】 特定の利用者グループにアクセスを制限して情報提供を行う W e b サーバ装置において、

前記特定の利用者グループにアクセスを制限した自装置のアクセス制限領域と同じアクセス制限領域を持ち認証情報を登録した他 W e b サーバを認証依頼先として登録した認証依頼先登録手段と、

クライアント端末からアクセスを限定したアクセス制限領域へのアクセス要求を受け、前記認証依頼先登録手段を参照して前記他 W e b サーバに対し認証依頼を行う認証依頼手段を有し、

前記第 2 W e b サーバからの認証結果を受け、前記認証結果に応じて前記クライアント端末からの前記アクセス制限領域のアクセスを行わせることを特徴とする W e b サーバ装置。

【請求項 4】 請求項 3 記載の認証装置において、

前記認証依頼手段は、他 W e b サーバから受けた認証情報要求を前記クライアント端末に渡し、

前記認証情報要求に対する前記クライアント端末から受けた認証情報を前記他 W e b サーバに渡すことを特徴とする認証装置。

【請求項 5】 請求項 1 記載の認証方法において、

前記第 2 W e b サーバは、複数の第 1 W e b サーバから認証依頼を行われることを特徴とする認証方法。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、認証方法及びその装置に関し、特に、複数の W e b サーバで特定の利用者グループにアクセスを制限するための認証方法及びその装置に関する。

【 0 0 0 2 】

【従来の技術】

W e b サーバによる情報利用が進むにつれ、ホームページによる情報提供を特定の利用者グループに限定し、複数の W e b サーバで特定の利用者グループに情報提供を行いたいという要求が急増している。

【 0 0 0 3 】

複数の W e b サーバに独立に登録され運用管理されるホームページに対して、特定の利用者グループにアクセスを限定した運用を行なうためには、各々の W e b サーバが同じ認証機能を所有している必要がある。

【 0 0 0 4 】

I D（識別番号）とパスワードによる利用者の認証は、現在、W e b サーバでは最もよく用いられている認証手段であるが、これを複数の W e b サーバで同じように利用するためには、アクセス制限を適用する全ての W e b サーバに同じ利用者の I D とパスワードのセットを登録しておく必要がある。または、固有のツールやシステムを使って利用者の I D とパスワードを共同利用する特別な仕組みが必要である。

【0 0 0 5】

I Dとパスワードを使用して複数のW e bサーバ上に特定の利用者グループからのアクセスのみを許可するホームページを掲載し運用する場合には、これまで次のような方法が取られて来た。

【0 0 0 6】

第1の方法は、利用者が全てのW e bサーバに認証情報（I Dとパスワード）を登録する。

【0 0 0 7】

第2の方法は、利用者はひとつのW e bサーバに自分の認証情報を登録し、他W e bサーバでは固有のツールやサーバ管理者によりコピーされた認証情報を使用する。

【0 0 0 8】

第3の方法は、W e bサーバを置くサーバシステム間で固有のツールやシステムを使って、各W e bサーバに登録された利用者の認証情報を相互利用する。

【0 0 0 9】

第4の方法は、利用者の認証情報を独立したサーバシステムに登録する。各W e bサーバがこのサーバシステム固有のツールを使い、利用者の認証情報を利用する。

【0 0 1 0】

【発明が解決しようとする課題】

従来の技術を使って、特定の利用者グループにアクセスを限定するホームページを独立した複数のW e bサーバで運用していくためには、次のような問題がある。

【0 0 1 1】

第1の方法で、各W e bサーバ上に利用者が認証情報（I Dとパスワード）を登録する場合、利用者は複数のW e bサーバで個々に登録操作を行う必要がある。利用者がI Dやパスワードの登録を間違えたり、忘れるといったことが起こり易い。また、各W e bサーバの管理者が個別に認証情報の管理を行う必要があり運用負荷が高くなるという問題があった。

## 【 0 0 1 2 】

第 2 の方法で、1 つの W e b サーバに全利用者の認証情報を登録し、これを他の W e b サーバ上にそのままコピーして使用する場合、確実にコピーを行なうためにサーバ管理者側の操作、あるいは個別のツールが必要となる。また、全ての W e b サーバ上の認証情報を時間遅れ無しでタイムリーに更新する仕組みは運用が難しいという問題があった。

## 【 0 0 1 3 】

第 3 の方法で、W e b サーバを置くサーバシステム間で互いに認証情報の共有する場合、各サーバ間で認証情報を共有するために固有のシステムが必要となる。また、この場合、各サーバ間の相互連携はシステムの運用を複雑にし、運用管面の負荷を増大させるという問題があった。

## 【 0 0 1 4 】

第 4 の方法で、利用者の認証情報を独立したサーバシステムで一括登録管理し、これを各 W e b サーバで利用する場合、各々の W e b サーバではこの独立したサーバシステムにアクセスするための固有のツールや機能が必要となる。例えばディレクトリサーバを使い認証情報を集中登録管理する場合には、ホームページのアクセス制限で使うために、さらに W e b サーバのどのページをどの利用者がアクセス可能か、といったような情報も別途登録して管理する必要があり、情報の登録管理及び運用方法ともに複雑になってしまうという問題があった。

## 【 0 0 1 5 】

例えば、LDAP ( L i g h t w e i g h t D i r e c t o r y A c c e s s P r o t o c o l ) を使ってディレクトリサーバに登録された利用者の情報を各 W e b サーバから利用する場合、ディレクトリサーバには認証情報や W e b サーバでアクセス制限を適用する領域やパターンに関する情報を登録しておかねばならない。

## 【 0 0 1 6 】

本発明は、上記の点に鑑みなされたものであり、複数の W e b サーバで特定の利用者グループにアクセスを制限するために、利用者の手間を低減でき、W e b サーバの運用管理の負担を少なくできる認証方法及びその装置を提供することを



目的とする。

【 0 0 1 7 】

【課題を解決するための手段】

請求項 1， 3 に記載の発明は、クライアント端末から特定の利用者グループにアクセスを限定した自装置のアクセス制限領域へのアクセス要求を受けた認証情報を持たない第 1 W e b サーバは、特定の利用者グループにアクセスを限定したアクセス制限領域を持ち認証情報を登録した第 2 W e b サーバに対し認証依頼を行い、第 2 W e b サーバからの認証結果を受けた第 1 W e b サーバは、認証結果に応じてクライアント端末からのアクセス制限領域のアクセスを行わせることにより、

複数の W e b サーバで特定の利用者グループにアクセスを制限するための利用者の手間を低減でき、 W e b サーバの運用管理の負担を少なくすることが可能となる。

【 0 0 1 8 】

請求項 2， 4 に記載の発明は、第 2 W e b サーバからの認証情報要求を受けた第 1 W e b サーバは、認証情報要求をクライアント端末に渡し、認証情報要求に対するクライアント端末からの認証情報を受けた第 1 W e b サーバは、認証情報を前記第 2 W e b サーバに渡すことにより、請求項 1 の発明を実現することが可能となる。

【 0 0 1 9 】

請求項 5 に記載の発明では、第 2 W e b サーバは、複数の第 1 W e b サーバから認証依頼を行われることにより、一つの第 2 W e b サーバで複数の第 1 W e b サーバから依頼された認証を行うことができる。

【 0 0 2 0 】

付記 6 に記載の発明では、第 1 W e b サーバは、複数の第 2 W e b サーバに対し認証依頼を行うことにより、利用者グループごとに異なる第 2 W e b サーバで認証を行うことが可能となる。

【 0 0 2 1 】

付記 7 に記載の発明では、第 1 W e b サーバは、他の第 1 W e b サーバに対し

認証依頼を行い、他の第1 Webサーバから第2 Webサーバに対し認証依頼を行うことにより、複数の第1 Webサーバを経て最後にたどり着く第2 Webサーバで認証を行うことが可能となる。

#### 【0022】

##### 【発明の実施の形態】

図1は、本発明の原理図を示す。同図中、認証依頼Webサーバ10は、本発明の機能を有するWebサーバであり、制御部12とページデータ部14とを有している。制御部12には、認証依頼機能13が設けられている。また、ページデータ部14には、認証依頼先URL定義領域15及びグループUのみアクセス可能なアクセス制限領域16が設けられている。

#### 【0023】

クライアント端末20のWebブラウザ22からは、利用者が認証依頼Webサーバ10にあるアクセス制限が適用されたホームページに対するアクセス要求が行われる。

#### 【0024】

マスターWebサーバ30は、通常のWebサーバを指すが、本明細書では特に認証依頼Webサーバ10と区別するためにこの名称を使用しており、マスターWebサーバ30とは、利用者が認証のために入力した認証情報（IDとパスワード）を既にユーザ登録簿35に登録済の認証情報と照合することにより、認証判定処理を行なうWebサーバを指す。マスターWebサーバ30は、制御部32とページデータ部34とを有している。制御部32には、認証判定処理を行なう認証機能33が設けられている。ページデータ部34には、ユーザ登録簿35と共に、グループUのみアクセス可能なアクセス制限領域36が設けられている。

#### 【0025】

認証依頼Webサーバ10は、通常のWebサーバであるマスターWebサーバ30が持つ機能に加えて、さらに次の2つの機能を持つ。第1の機能は、認証依頼先URL定義領域15であり、アクセス制限を適用する自Webサーバ上のアクセス制限領域16に対応させて設けている。認証依頼先URL定義領域15

には自Webサーバ上で適用したいアクセス制限と同じアクセス制限を使用して  
いる他Webサーバのアクセス制限領域（例えばマスターWebサーバ30の  
アクセス制限領域36）を参照するためのURL（Uniform Resource  
Locator）が登録されている。

## 【0026】

第2の機能は、認証依頼先URL定義領域15から読み出された該当の他Web  
サーバのURLにアクセスすることで認証の可否を確認する認証依頼機能13  
である。認証依頼機能13は、自Webサーバ上の当該アクセス制限下にあるア  
クセス制限領域16のホームページに利用者がアクセスした場合、利用者が入力  
するIDとパスワードを使って他サーバ（例えばマスターWebサーバ30）に  
アクセスし、その認証の可否を決定する機能を持つ。

## 【0027】

以上の2つの機能により、自Webサーバ上に直接、利用者の認証情報を持っ  
ていない場合でも、他Webサーバの認証機能を使うことで、自Webサーバに  
アクセス制限を適用したホームページを提供できる。

## 【0028】

なお、認証依頼Webサーバ10は、通常のWebサーバであるマスターWeb  
サーバ30が持つ機能も持っているため、自Webサーバ上のアクセス制限さ  
れていない領域のホームページに利用者がアクセスした場合は、この領域からア  
クセスされたホームページを読み出した利用者に提供する。

## 【0029】

図2を用いて利用者が自分の属するグループUのみアクセスを許可されている  
アクセス制限領域16内のページ（data.html）の取得を要求した場合  
の処理の流れを説明する。

## 【0030】

ここで、利用者の認証情報はマスターWebサーバ30のユーザ登録簿35に  
のみ登録されており、認証依頼Webサーバ10には存在しない。マスターWeb  
サーバ30でグループUのみアクセスを許可されているアクセス制限領域36  
内のページのひとつを“/secret/check.html”とする。

【0031】

認証依頼Webサーバ10には、このページのURL “AAA. com//secret/check. html” が、グループUのみアクセスを許可されているアクセス制限領域16と対応させて、認証依頼先URL定義領域15に登録されている。

【0032】

認証依頼機能13は利用者から要求されたページの属するアクセス制限領域16に対応して認証依頼先URL定義領域15が存在する場合には、自Webサーバでの認証処理を行わずに、認証依頼先URL定義領域15で指定されたURL “AAA. com//secret/check. html” のアクセスによりマスターWebサーバ30を利用した認証処理を行なう。

【0033】

①クライアント端末20は、認証依頼Webサーバ10上のアクセス制限領域16にあるアクセス制限されたページ [data. html] の取得を要求する。

【0034】

②認証依頼Webサーバ10の認証依頼機能13は、要求されたページがあるアクセス制限領域16に対応した認証依頼先URL定義領域15が存在するか否かを調べ、存在する場合には認証依頼先URL定義領域15から読み出したURL “AAA. com//secret/check. html” にアクセスする。ここでは、HTTPプロトコルでのページ要求、あるいはページ更新チェックなどのコマンドを用いる。

【0035】

③マスターWebサーバ30は、アクセス制限領域36にあるURL “AAA. com//secret/check. html” のアクセスなので認証依頼Webサーバ10の認証依頼機能13に対してIDとパスワードを要求する。

【0036】

④認証依頼Webサーバ10は、利用者に対してマスターWebサーバから要求された形式のIDとパスワードの入力を要求する。

【 0 0 3 7 】

⑤利用者は、WEBブラウザ22から要求されたIDとパスワードを入力する。

【 0 0 3 8 】

⑥認証依頼機能13は、WEBブラウザ22から供給される上記IDとパスワードをマスターWebサーバ30に返す。

【 0 0 3 9 】

⑦認証機能33は、認証OKの場合その旨の応答を認証依頼Webサーバ10に返す。

【 0 0 4 0 】

⑧認証依頼Webサーバ10は認証OKの応答により、利用者に最初に要求されたdata.htmlをアクセス制限領域16から読み出し、WEBブラウザ22に渡す。

【 0 0 4 1 】

図3に、認証依頼機能13での制御の流れを自サーバで認証処理を行う場合の制御の流れと対比させて示す。同図中、アクセス制限を適用したページの取得要求があると、実線の矢印で示すように、認証依頼機能13はステップS10で要求ページに該当するマスターWebサーバ30のURLにアクセスする。そして、マスターWebサーバ30からIDとパスワードの要求を受けると、ステップS12でこの要求をWEBブラウザ22に渡す。WEBブラウザ22からIDとパスワードが供給されると、ステップS14でこのIDとパスワードをマスターWebサーバ30に渡し、認証OKの応答を受けると要求ページをWEBブラウザ22に渡す。

【 0 0 4 2 】

これに対し、自サーバで認証処理を行う場合、アクセス制限を適用したページの取得要求があると、破線の矢印で示すように、自サーバはステップS20でIDとパスワードをWEBブラウザ22に要求する。WEBブラウザ22からIDとパスワードが供給されると、ステップS22でこのIDとパスワードを自サーバ内のユーザ登録簿と照合し、認証OKの場合にステップS24で自サーバから

要求ページをWEBブラウザ22に渡す。

【0043】

図4を用いて他Webサーバの参照処理を再帰的に使用する実施例について説明する。同図中、クライアント端末20から認証依頼Webサーバ10上のアクセス制限領域16にあるアクセス制限されたページの取得要求が行われ、認証依頼Webサーバ10から認証依頼を受けたWebサーバが認証依頼Webサーバ40であった場合、この認証依頼Webサーバ40は次のWebサーバに認証依頼を出す。この認証依頼は一または複数の認証依頼Webサーバ40を経てマスターWebサーバ30に渡される。

【0044】

その後、マスターWebサーバ30からのIDとパスワードの要求は上記認証依頼とは逆の経路で認証依頼Webサーバ40, 10を経てクライアント端末20に渡され、これに対するクライアント端末20の応答(IDとパスワード)は認証依頼Webサーバ10, 40を経てマスターWebサーバ30に渡される。そして、マスターWebサーバ30からの認証OKの応答が認証依頼Webサーバ40から認証依頼Webサーバ10に渡され、認証依頼Webサーバ10は要求ページをクライアント端末20に渡す。

【0045】

このように経路内に複数の認証依頼Webサーバ10, 40がある場合にも、実際に利用者が入力したIDとパスワードを既に登録されている認証情報と照らし合わせる認証処理を行なうのは、最後にたどり着くマスターWebサーバ30である。

【0046】

図5(A), (B), (C)に認証依頼Webサーバの基本的な構成パターンを示す。図5(A)のパターンでは、1つのマスターWebサーバ30を複数の認証依頼Webサーバ10a~10cからアクセスして利用する。

【0047】

図5(B)のパターンでは、1つの認証依頼Webサーバ10から複数のマスターWebサーバ30a~30cを参照する。この場合、認証依頼Webサーバ1

0 上に、それぞれ異なるアクセス制限を適用するアクセス制限領域 1 6 a, 1 6 b, 1 6 c 各々に対して認証依頼先 URL 定義領域 1 5 a, 1 5 b, 1 5 c を設け、それぞれによりマスタ Web サーバ 3 0 a ~ 3 0 c を参照する。

【 0 0 4 8 】

図 5 (C) のパターンでは、認証依頼 Web サーバ 1 0 が認証を依頼する Web サーバが認証依頼 Web サーバ 4 0 であり、認証依頼 Web サーバ 4 0 からマスタ Web サーバ 2 0 に認証を依頼する。図 4 と同一構成であり、認証依頼 Web サーバ 4 0 が複数段従属接続されてもよい。

【 0 0 4 9 】

図 6 は、本発明の第 1 実施例のシステム構成図を示す。このシステムは会社内に構築される。本社の Web サーバ 5 0 がマスター Web サーバとされ、この Web サーバ 5 0 上には経理関係者のみがアクセス可能なアクセス制限領域 5 6 が定義されると共に、本社と支社を含む会社の全経理関係者の ID とパスワードを登録したユーザ登録簿 5 5 が設けられている。

【 0 0 5 0 】

各支店の Web サーバ 6 0, 7 0 は認証依頼 Web サーバとして構成されており、各支店で作成登録した経理関係者のみにアクセスを限定するホームページの開設は、本社の Web サーバ 5 0 のアクセス制限領域 5 6 を参照することで可能となる。各支店の Web サーバ 6 0, 7 0 それぞれで個別に認証のための ID とパスワードの登録は必要がない。

【 0 0 5 1 】

本社 Web サーバ 5 0 のアクセス制限領域 5 6 に属する任意の URL が公開されていれば、各支店ではこれを支店の Web サーバに登録するだけで、本社の Web サーバで実施しているのと同じのアクセス制限条件下（経理関係者の ID とパスワード）でアクセス制限領域 6 6, 7 6 にてホームページを提供することが可能となる。

【 0 0 5 2 】

経理関係者はクライアント端末 8 0 から ID とパスワードを入力することにより、Web サーバ 5 0, 6 0, 7 0 それぞれのアクセス制限領域 5 6, 6 6, 7

6 のホームページをアクセスすることができる。

【 0 0 5 3 】

図 7 は、本発明の第 2 実施例のシステム構成図を示す。このシステムは公共施設の W e b サーバで実施される。市役所の W e b サーバ 8 0 では各種団体やグループが自分達のホームページを開設することを認めており、この W e b サーバ 8 0 を認証依頼 W e b サーバで構成する。

【 0 0 5 4 】

そして、政党本部 W e b サーバ 9 0、県庁 W e b サーバ 1 0 0、趣味の会 W e b サーバ 1 1 0 それぞれをマスター W e b サーバで構成し、各 W e b サーバ 9 0、1 0 0、1 1 0 それぞれに、政党関係者全員の I D とパスワードを登録したユーザ登録簿 9 5、県職員全員の I D とパスワードを登録したユーザ登録簿 1 0 5、趣味の会の会員全員の I D とパスワードを登録したユーザ登録簿 1 1 5 を設ける。

【 0 0 5 5 】

市役所の W e b サーバ 8 0 には、各種団体やグループそれぞれだけがアクセス可能なアクセス制限領域 8 6 a、8 6 b、8 6 c とこれに対応する認証依頼先 U R L 定義領域を定義し、アクセス制限領域 8 6 a、8 6 b、8 6 c それぞれに各グループのホームページを設ける。

【 0 0 5 6 】

これにより、各種団体やグループそれぞれは、クライアント端末 1 2 0、1 2 2 から市役所の W e b サーバ 8 0 に接続し、W e b サーバ 8 0 から各々のマスター W e b サーバである W e b サーバ 9 0、1 0 0、1 1 0 の該当 U R L を参照して各グループの I D とパスワードの認証を行い、アクセスを制限したアクセス制限領域 8 6 a、8 6 b、8 6 c に設定した各グループのホームページを閲覧することができる。

【 0 0 5 7 】

図 8 に、認証依頼先 U R L 定義の一実施例を示す。図 8 では、左側の認証依頼 W e b サーバ 1 0 で定義する認証依頼先 U R L 定義ファイル “. h t a c c e s s \_ \_ E” を、右側の U N I X（登録商標）で動作する従来の W e b サーバで使用



されているアクセス制限定義ファイル “. h t a c c e s s ファイル” と比較して示している。両方ともアクセス制限を適用するアクセス制限領域の最上位のディレクトリ配下に設置して使用する。なお、図中、上段は定義形式、下段は定義例を示す。

## 【 0 0 5 8 】

認証依頼先URL定義ファイル “. h t a c c e s s \_ E ” でのパラメタは次のように定義されている。A u t h U R L は認証処理のために参照するサーバのURLを記述する。A u t h N a m e は認証に与える名称（利用者のブラウザの表示で見せるためのものなので任意に設定できる）である。A u t h T y p e は認証手法であり、ここでは定義しない。マスターW e b サーバから指定された認証手法を使って利用者にIDとパスワードを要求するので、この情報は認証依頼機能で判定、設定して使用する。

## 【 0 0 5 9 】

本発明によれば、ホームページ利用者にとっては、マスターW e b サーバ30となるサーバにだけ自分のIDとパスワードを登録すればよく、複数のW e b サーバに何度もIDやパスワードを入れる手間がなくなり、自分のIDとパスワードを忘れて困る、ということも少なくなる。

## 【 0 0 6 0 】

また、ホームページ開設者にとっては、自分達のグループにアクセスを限定したホームページを身近なW e b サーバを使って開設することが容易にでき、グループ内でのホームページでの情報提供を分担して行うことが容易となる。更に、IDとパスワードが一箇所での集中管理となるので、複数のサーバで登録管理する場合に比べて認証情報を運用管理する者の負担が少なくなる。

## 【 0 0 6 1 】

また、W e b サーバ管理者にとっては、マスターW e b サーバ側の管理者はこれを参照する認証依頼W e b サーバの存在を意識する必要はない。W e b サーバ間での認証情報交換のための特別なシステムも不要なので運用での新たな負荷は発生しない。また、連携に必要なURL情報は公開しても差し支えない性格のものであるので、広報、伝達時の情報の扱いが簡単である。更に、自W e b サーバ上で

の I D とパスワード管理と併用可能なので、通常の W e b サーバから認証依頼 W e b サーバに移行した場合でも従来通りの運用は全く影響を受けない。

なお、認証依頼 W e b サーバ 1 0 が請求項記載の第 1 W e b サーバに対応し、マスター W e b サーバ 3 0 が第 2 W e b サーバに対応し、認証依頼先 U R L 定義領域 1 5 が認証依頼先登録手段に対応し、認証依頼機能 1 3 が認証依頼手段に対応する。

【 0 0 6 2 】

(付記 1) 複数の W e b サーバで特定の利用者グループにアクセスを制限するための認証方法において、

クライアント端末から前記特定の利用者グループにアクセスを限定した自装置のアクセス制限領域へのアクセス要求を受けた認証情報を持たない第 1 W e b サーバは、前記特定の利用者グループにアクセスを限定したアクセス制限領域を持ち認証情報を登録した第 2 W e b サーバに対し認証依頼を行い、

前記第 2 W e b サーバからの認証結果を受けた前記第 1 W e b サーバは、前記認証結果に応じて前記クライアント端末からの前記アクセス制限領域のアクセスを行わせることを特徴とする認証方法。

【 0 0 6 3 】

(付記 2) 付記 1 記載の認証方法において、

前記第 2 W e b サーバからの認証情報要求を受けた前記第 1 W e b サーバは、前記認証情報要求を前記クライアント端末に渡し、

前記認証情報要求に対する前記クライアント端末からの認証情報を受けた前記第 1 W e b サーバは、前記認証情報を前記第 2 W e b サーバに渡すことを特徴とする認証方法。

【 0 0 6 4 】

(付記 3) 特定の利用者グループにアクセスを制限して情報提供を行う W e b サーバ装置において、

前記特定の利用者グループにアクセスを制限した自装置のアクセス制限領域と同じアクセス制限領域を持ち認証情報を登録した他 W e b サーバを認証依頼先として登録した認証依頼先登録手段と、

クライアント端末からアクセスを限定したアクセス制限領域へのアクセス要求を受け、前記認証依頼先登録手段を参照して前記他 W e b サーバに対し認証依頼を行う認証依頼手段を有し、

前記第 2 W e b サーバからの認証結果を受け、前記認証結果に応じて前記クライアント端末からの前記アクセス制限領域のアクセスを行わせることを特徴とする W e b サーバ装置。

【 0 0 6 5 】

(付記 4) 付記 3 記載の認証装置において、

前記認証依頼手段は、他 W e b サーバから受けた認証情報要求を前記クライアント端末に渡し、

前記認証情報要求に対する前記クライアント端末から受けた認証情報を前記他 W e b サーバに渡すことを特徴とする認証装置。

【 0 0 6 6 】

(付記 5) 付記 1 記載の認証方法において、

前記第 2 W e b サーバは、複数の第 1 W e b サーバから認証依頼を行われることを特徴とする認証方法。

【 0 0 6 7 】

(付記 6) 付記 1 記載の認証方法において、

前記第 1 W e b サーバは、複数の第 2 W e b サーバに対し認証依頼を行うことを特徴とする認証方法。

【 0 0 6 8 】

(付記 7) 付記 1 記載の認証方法において、

前記第 1 W e b サーバは、他の第 1 W e b サーバに対し認証依頼を行い、

前記他の第 1 W e b サーバから前記第 2 W e b サーバに対し認証依頼を行うことを特徴とする認証方法。

【 0 0 6 9 】

【発明の効果】

上述の如く、請求項 1, 3 に記載の発明によれば、複数の W e b サーバで特定の利用者グループにアクセスを制限するための利用者の手間を低減でき、 W e b

サーバの運用管理の負担を少なくすることが可能となる。

【 0 0 7 0 】

また、請求項 2， 4 に記載の発明によれば、請求項 1 の発明を実現することが可能となる。

【 0 0 7 1 】

また、請求項 5 に記載の発明によれば、一つの第 2 W e b サーバで複数の第 1 W e b サーバから依頼された認証を行うことができる。

【 0 0 7 2 】

また、付記 6 に記載の発明によれば、利用者グループごとに異なる第 2 W e b サーバで認証を行うことが可能となる。

【 0 0 7 3 】

また、付記 7 に記載の発明によれば、複数の第 1 W e b サーバを経て最後にたどり着く第 2 W e b サーバで認証を行うことが可能となる。

【図面の簡単な説明】

【図 1】

本発明の原理図である。

【図 2】

アクセス制限領域内のページの取得を要求した場合の処理の流れを説明するための図である。

【図 3】

認証依頼機能での制御の流れを自サーバで認証処理を行う場合の制御の流れと対比させて示す図である。

【図 4】

他 W e b サーバの参照処理を再帰的に使用する実施例を説明するための図である。

【図 5】

認証依頼 W e b サーバの基本的な構成パターンを示す図である。

【図 6】

本発明の第 1 実施例のシステム構成図である。

【図 7】

本発明の第 2 実施例のシステム構成図である。

【図 8】

認証依頼先 URL 定義の一実施例を示す図である。

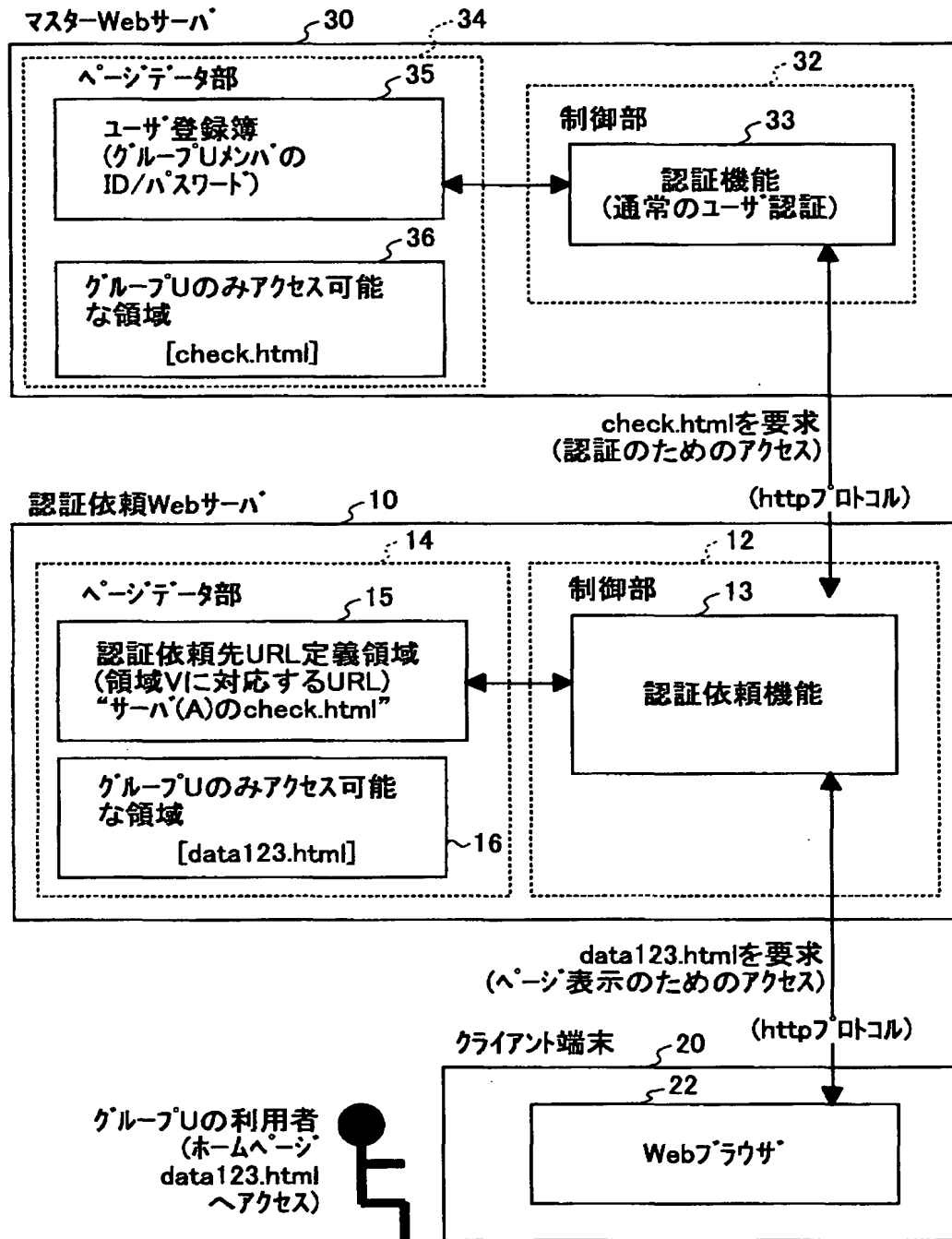
【符号の説明】

- 1 0 認証依頼 W e b サーバ
- 1 2 制御部
- 1 3 認証依頼機能
- 1 4 ページデータ部
- 1 5 認証依頼先 URL 定義領域
- 1 6 アクセス制限領域
- 2 0 クライアント端末
- 2 2 W e b ブラウザ
- 3 0 マスター W e b サーバ
- 3 2 制御部
- 3 4 ページデータ部
- 3 5 ユーザ登録簿
- 3 6 アクセス制限領域

【書類名】 図面

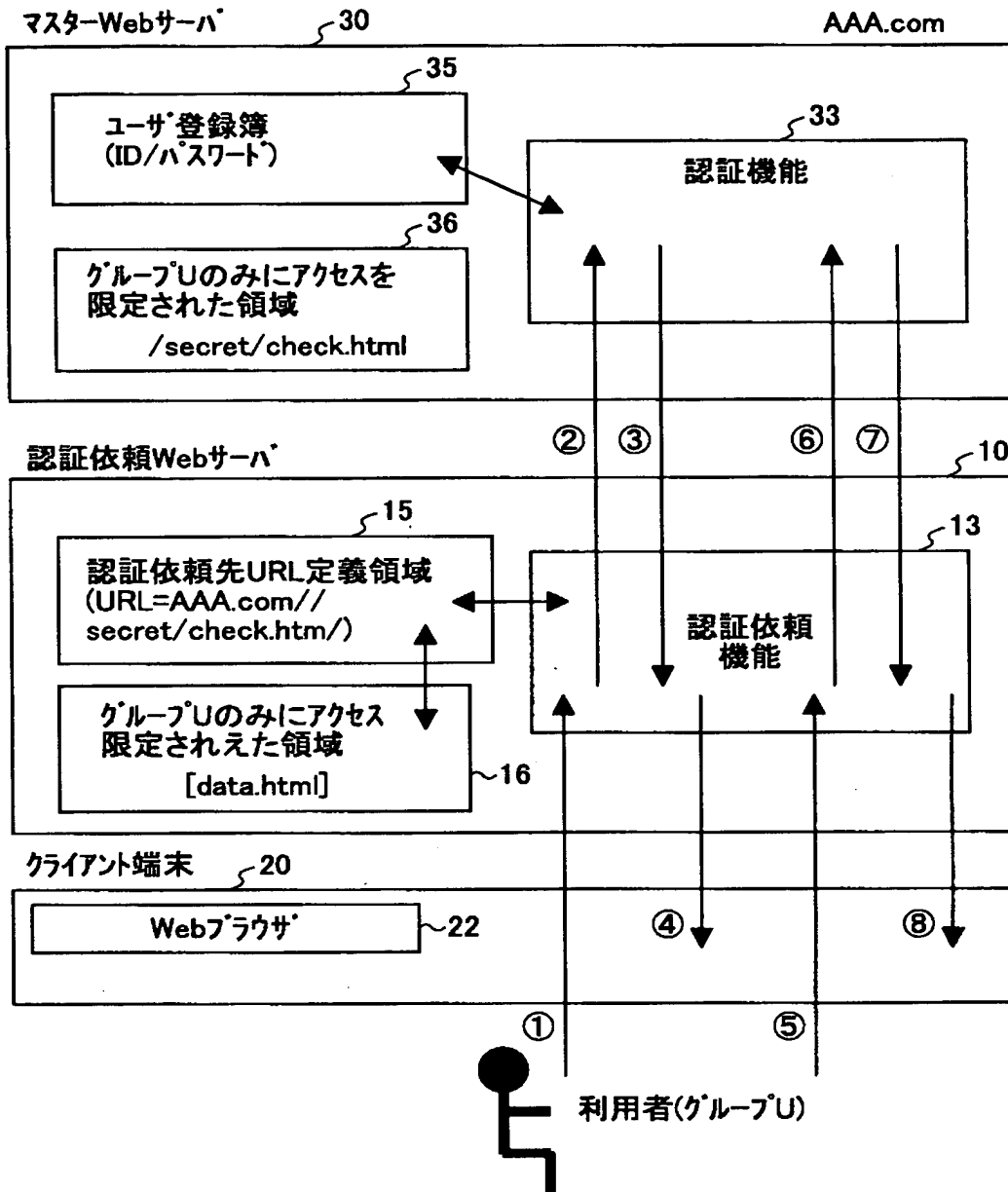
【図1】

本発明の原理図



【図 2】

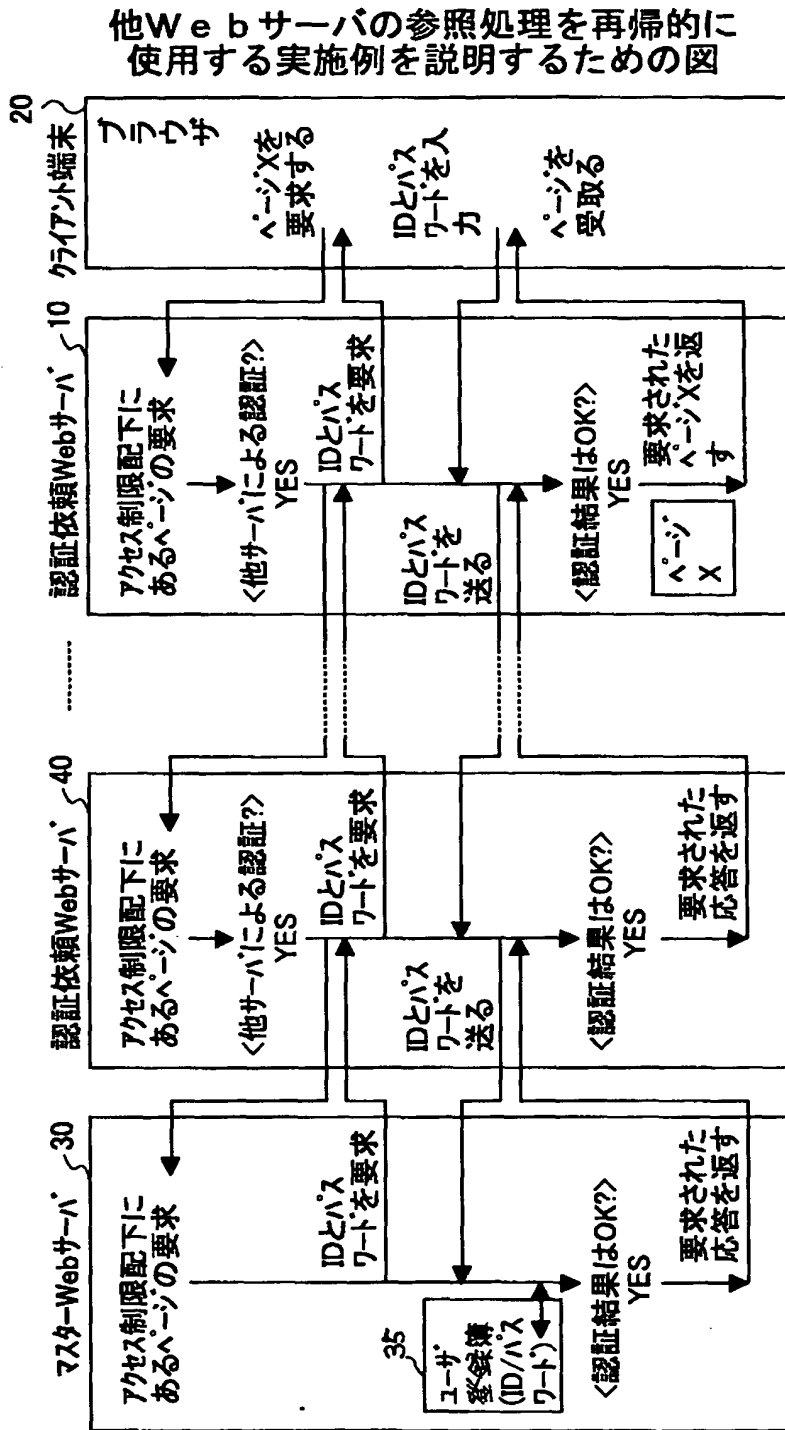
アクセス制限領域内のページの取得を要求した場合の処理の流れを説明するための図





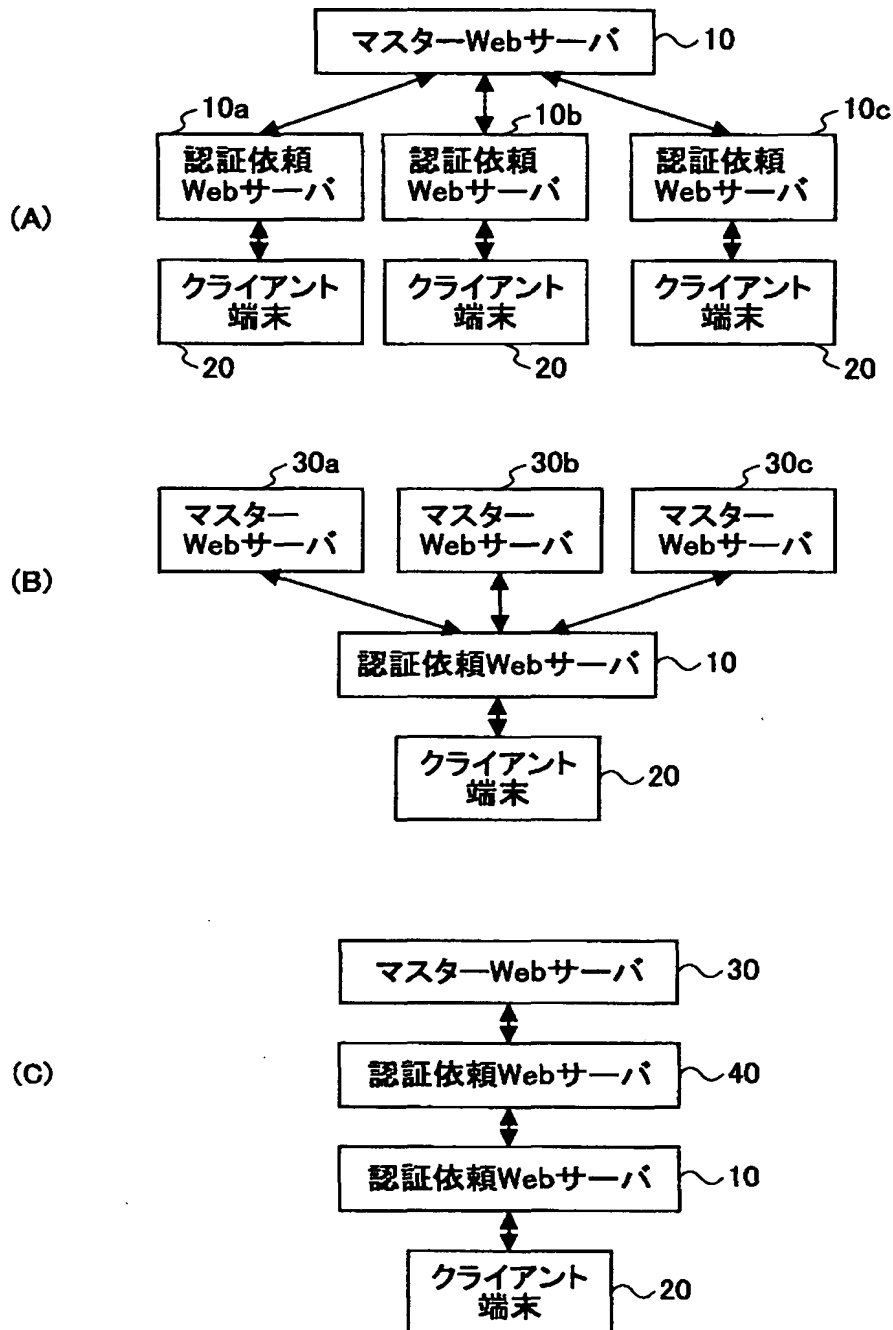


【図 4】



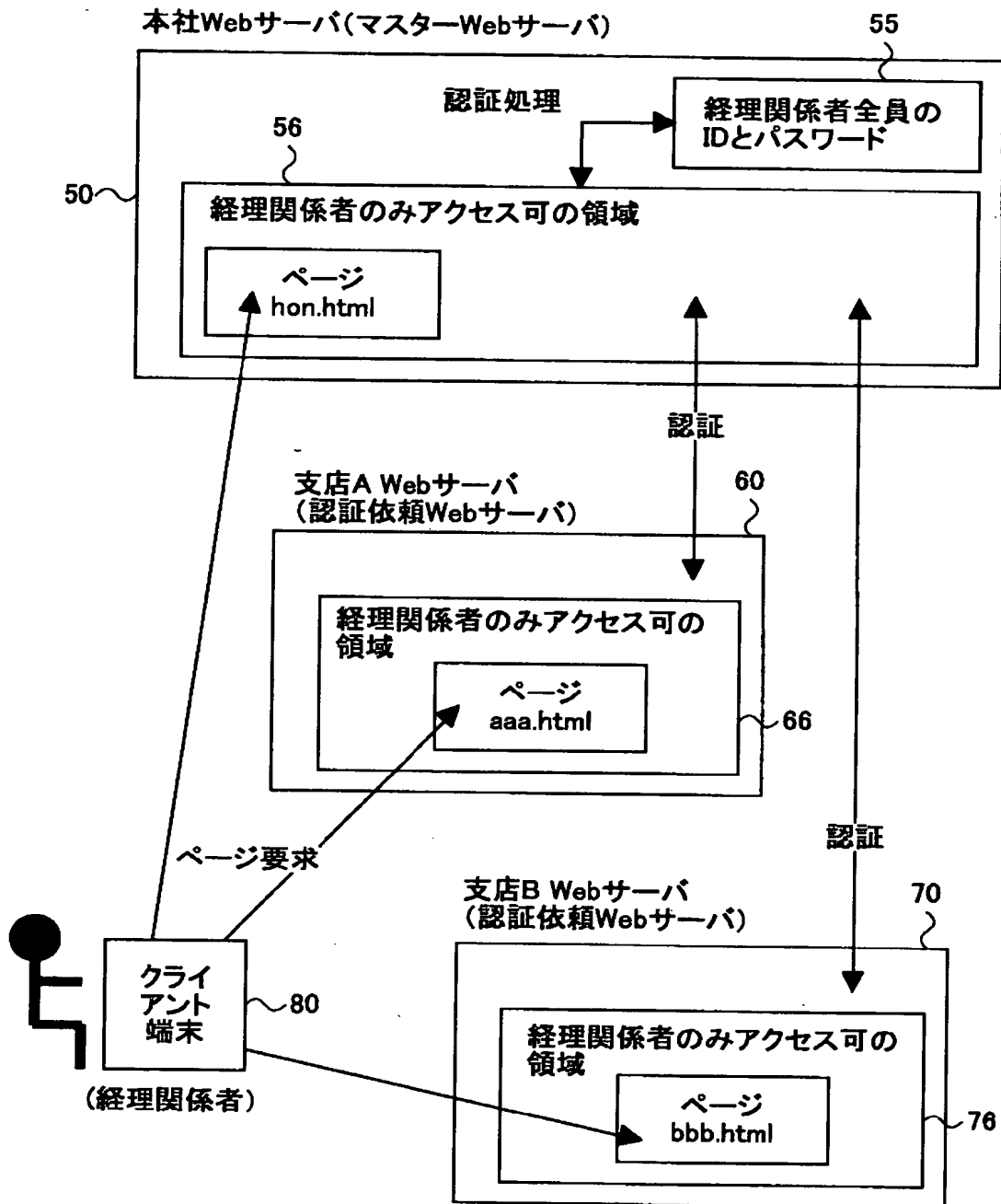
【図 5】

認証依頼Webサーバの基本的な構成パターンを示す図



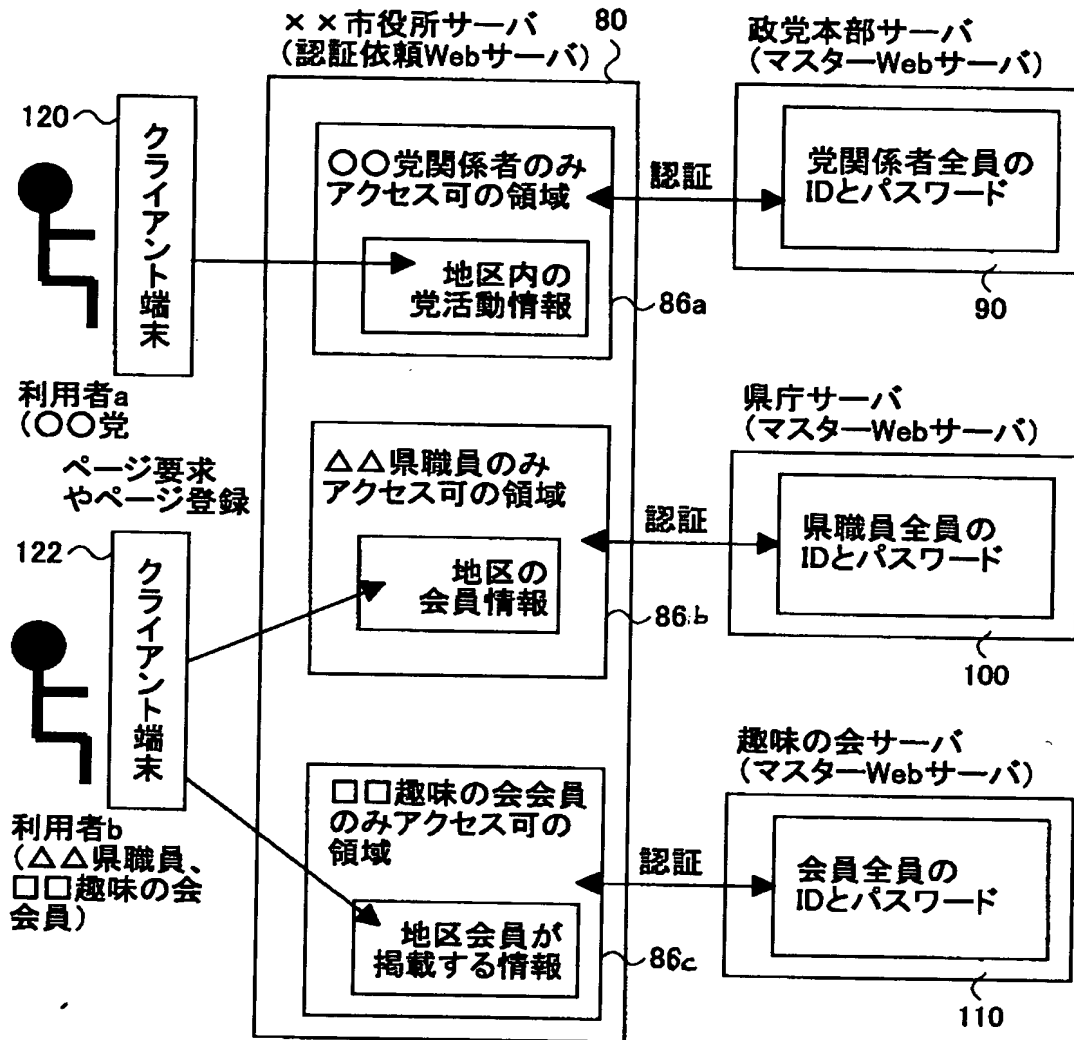
【図 6】

本発明の第 1 実施例のシステム構成図



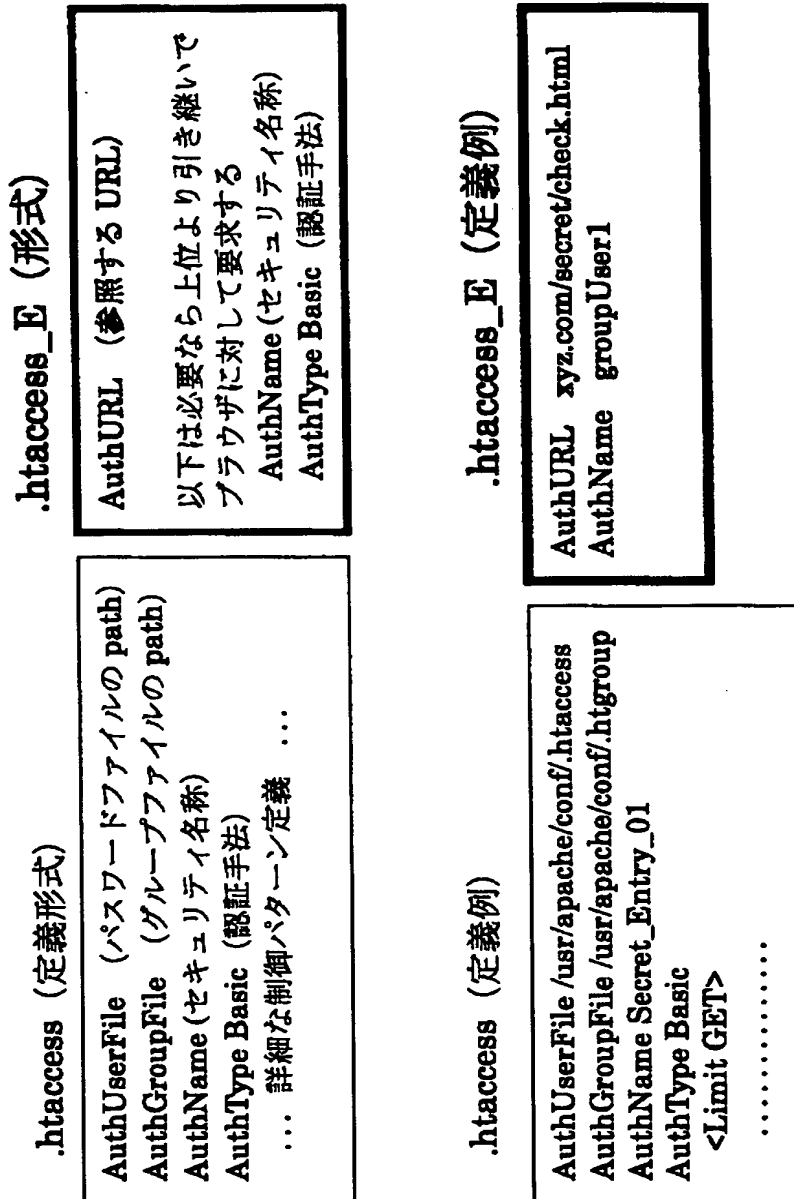
【図 7】

本発明の第 2 実施例のシステム構成図



【図 8】

認証依頼先 URL 定義の一実施例を示す図



【書類名】 要約書

【要約】

【課題】 本発明は、複数のW e bサーバで特定の利用者グループにアクセスを制限するために、利用者の手間を低減でき、W e bサーバの運用管理の負担を少なくできる認証方法及びその装置を提供することを目的とする。

【解決手段】 クライアント端末2 0 から自装置のアクセス制限領域へのアクセス要求を受けた認証情報を持たない第1 W e bサーバ1 0 は、特定の利用者グループにアクセスを限定したアクセス制限領域を持ち認証情報を登録した第2 W e bサーバ3 0 に対し認証依頼を行い、第2 W e bサーバからの認証結果を受けた第1 W e bサーバは、認証結果に応じてクライアント端末からのアクセス制限領域のアクセスを行わせることにより、利用者の手間を低減でき、W e bサーバの運用管理の負担を少なくすることが可能となる。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [ 0 0 0 0 0 5 2 2 3 ]

1. 変更年月日	1 9 9 6 年 3 月 2 6 日
[変更理由]	住所変更
住 所	神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号
氏 名	富士通株式会社